YOUTH SERVICES
POLICY

Title: Access to, Security of, and Use of Information Technology Resources and Mobile Devices **Next Annual Review Date:** 08/04/2012	**Type:** A. Administrative **Sub Type:** 5. Information Services **Number:** A.5.1
	Page 1 **of** 6
References: ACA Standards 2-CO-1E-01 (Administration of Correctional Agencies), 4-JCF-6F-04 and 4-JCF-6F-07 (Performance-Based Standards For Juvenile Correctional Facilities); CJCA Performance-Based Standard PP24; YS Policies A.3.1 "Asset Management", A.3.3 "Requests for Statistical Information; Collection of Fees for Reproduction of Public Records and Statistical Reports", A.5.10 "Information Technology (IT) Technical Support", B.3.2 “Access to and Release of Active and Inactive Youth Records”, C.1.5 "Research" and C.1.13 "Legislative Request/Communication, Media Access and Public Information"; and OIT ITStandard 6-01 Desktop Confirguation	
STATUS: Approved	
Approved By: *Mary L. Livers, Deputy Secretary*	**Date of Approval:** 08/04/2011

I. AUTHORITY:

Deputy Secretary of Youth Services (YS) as contained in La. R.S. 36:405. Deviation from this policy must be approved by the Deputy Secretary.

II. PURPOSE:

To establish access to and use of YS information systems, to ensure compliance with federal regulations governing privacy and security of information, and to protect confidential data in the event of computer equipment or mobile electronic data device loss and/or theft.

III. APPLICABILITY:

This policy applies to all employees of YS. Each Unit Head is responsible for ensuring that all necessary procedures are in place to comply with the provisions of this policy.

IV. DEFINITIONS:

Computer Equipment - Includes computer file servers, desktop/notebook computers, data communications equipment, personal digital assistants (PDA), and Smart Phones.

Confidential Data - Includes information protected by Federal, State, and/or local statutes, regulations, YS policies, or contractual language. Managers may also designate data as Confidential. Any disclosure of Confidential Data must be authorized by the Deputy Secretary. For illustration purposes only, some examples of Confidential Data include:

Medical records;
Youth records and other non-public youth data;
Social Security numbers;

Bank account numbers and other personal financial information;
Personnel and/or payroll records; and
Any data identified by government or YS policies to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Information Systems - YS and Public Safety Services (PSS) information systems that reside on computer equipment located within IT; includes hardware and software components.

Mobile Electronic Data Device - Any electric and/or battery operated device that can be easily transported, and that has the capability for storing, processing and/or transmitting data, including but not limited to laptops, mini hard drives, back-up hard drives, Zip Drives, Flash Drives, Personal Data Assistants (i.e. PDAs, including but not limited to, Smart Phones, Hand Held PCs), or any other mobile device designed or modified to store, process and/or transmit data.

Security - Those precautions and safeguards that are used to protect the integrity of, and prohibit unauthorized access to, the data stored in the information systems. This includes computer user-IDs and passwords, computer user access rights, information system time-out parameters, restricted office access, and locked offices.

Unauthorized Access - Ability to view, add, modify, delete, print, copy, or transmit data from an information system where the individual gaining access does not have the right or the need to know such information.

Unit Head - Deputy Secretary, Assistant Secretary, Undersecretary, Chief of Operations, Deputy Assistant Secretaries, Facility Directors, and Regional Managers.

YS Central Office - Offices of the Deputy Secretary, Assistant Secretary, Undersecretary, Chief of Operations, Deputy Assistant Secretaries and their support staff.

V. POLICY:

It is the Deputy Secretary's policy to make computers available to employees to perform their job duties. Computers must be used for official business only. All other uses are strictly prohibited. Access to an employee's computer by youth in the custody or under the supervision of YS is strictly prohibited, except for instructional use at schools/libraries within the secure care facilities.

All YS staff utilizing a computer or mobile electronic data device (e.g. Laptop, Flash Drive, Smart Phone, Hand Held PC, etc.) is responsible for the data stored, processed and/or transmitted via that computer or device, and for following the security requirements set forth in this policy.

VI. PROCEDURES:

A. Assignment of Computer Equipment and Mobile Electronic Devices

Requests for computer equipment or other mobile electronic devices shall be submitted through the appropriate Unit Head to the Public Safety Services (PSS) Helpdesk at (225) 925-6233, with a copy forwarded to the YS IT Director. Immediate supervisor or Unit Head approval shall be based on the work needs of the employee. A "Movable Property" form (refer to YS Policy A.3.1) shall be completed and signed by the employee when the computer equipment or mobile electronic device is delivered.

The PSS Information Technology (IT) Director shall not authorize the assignment of any computer equipment or mobile electronic device without the approval of the YS IT Director and the Unit Head.

B. Access to Information Technology Systems

1. Each employee authorized to use an IT system shall be assigned a unique computer-user ID and password, and shall be given the level of access necessary to complete their job duties or functions as determined by the employee's Unit Head.

2. Each unit and/or the PSS or YS IT Director shall provide training on access to and use of JETS and other information systems.

C. Use of Information Technology Systems

1. YS and PSS IT Systems facilitate decision-making, research, and timely responses to youth needs and information requests. This includes the exchange of information between all units, including law enforcement and criminal justice agencies, while respecting the confidentiality and privacy of youth records.

2. Data from IT systems shall be used for reporting statistics and general demographic information to all employees of YS, government agencies, legislative staff, media, and the general public. (Refer to YS Policies A.3.3 and C.1.13)

3. Dissemination of information shall be based on the right and need to know of the person(s) making the request, thus prohibiting unauthorized access and/or dissemination of criminal record information without authorization. (Refer to YS Policies A.3.3, C.1.13, and B.3.2)

4. Appropriate computer software necessary for the employee to perform their assigned job duties shall be installed on an employee's assigned computer. Personal software is strictly prohibited without the authorization of the YS and PSS IT Directors, in accordance with YS Policy A.5.10.

5. Software from outside vendors of other governmental agencies may be installed, with approval from the IT Director, to meet an internal need or to participate in a multi-agency initiative. The use of such software must not compromise YS' computer security infrastructure. Any violation of policies established for the use of such software, resulting in the disclosure of classified information to unauthorized persons, injury or loss to the system, unauthorized modification or destruction of system data, or loss by theft of any computer system media, may result in disciplinary action. Software installation approvals by the YS IT Director shall be copied to the PSS IT Director.

6. Employees are prohibited from changing a computer's hardware or system settings, opening the computer case to remove, replace, or repair components, or having computer administrator rights to their assigned computer unless authorized by the PSS and IT Directors.

7. All computer equipment and mobile devices must conform to applicable Division of Administration, Office of Information Technology Standards. The YS IT Director is responsible for ensuring the dissemination of applicable standards to all units.

8. Employees must report state tag numbers, and be able to produce computer equipment and mobile devices, when requested by inventory control staff.

9. Employees shall not provide their passwords to anyone. Public Safety Services IT and YS IT staff may request an employee's password in order to troubleshoot a problem under the employee's ID. If PSS or YS IT staff request a password, once they are finished the employee must change their password.

10. All computer software products used throughout YS for email, anti-virus, and the information systems, must have a registered license through PSS IT.

11. All Windows desktop/notebook computers must be configured for automatic Windows Updates.

12. A minimum of once every two (2) weeks, all employees assigned the use of a notebook or laptop computer shall ensure the equipment is turned on and attached to the network for a minimum of one (1) hour, to allow anti-virus and operation system updates.

13. A minimum of once per month, or when Microsoft issues a security threat alert, all Windows file servers and computers must be updated by PSS IT with the latest Windows Updates.

14. Each Unit Head shall appoint staff to coordinate with the YS IT Director in developing priority lists for improvements to existing information systems, and the development and design of new information systems.

D. Protection of Confidential Data on Computer Equipment

1. Information stored on computer equipment is the property of the State of Louisiana. All information that Unit Heads determine to be critical to their operations must be saved on a regular basis to a removable (computer tape, CD, external hard drive, etc.), and stored in a secured area or saved to a fixed media, such as a dedicated back-up file server.

2. All desktop/notebook computers must be configured to activate the screen saver password protect feature upon a maximum of 30 minutes with no keyboard/mouse activity.

E. Protection of Confidential Data on Laptops or Electronic Data Mobile Devices

1. A laptop or other electronic data mobile device must authenticate the user before access to services on or by the device are permitted. Mobile devices must be configured to time-out after 15 minutes of inactivity, and require re-authentication before access to services on or by the device will be permitted. The authentication mechanism(s) must not be disabled.

2. The encryption option must be enabled on laptop computers that transmit or store confidential information. Laptops shall be protected with antivirus software, and updated daily if supported by the device.

   NOTE: YS e-mail is protected with centralized anti-virus and anti-spam software through PSS IT. This protection may not apply to emails systems outside of YS.

3. The use of unprotected mobile devices to access or store Confidential Data is prohibited regardless of whether the equipment is owned or managed by PSS or YS, and shall result in disciplinary action.

F. Reporting Loss/Theft of Equipment or Data

Employees are expected to secure computer equipment when left unattended. Any lost or stolen equipment shall be reported immediately to the YS IT Director, who shall advise the PSS IT Director.

G. Termination of Access to Information Technology Resources

1. Upon an employee's end of service with YS, the PSS Helpdesk and the YS IT Director shall be informed by the immediate supervisor and/or HR staff of the employee's departure date.

2. The PSS Helpdesk and YS IT Director, upon notification, shall terminate all access to YS computer equipment, databases, and/or electronic data mobile devices, effective on the employee's separation date.

3. The Unit Head may, at any time prior to the separation date, request termination of an employee's access if the situation warrants such action.

4. The YS IT Director shall maintain a record of all requests for termination of access.

Previous Regulation/Policy Number: A.5.1
Previous Effective Date: 4/26/11
Attachments/References: